



DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2023-0008]

Agency Information Collection Activities:

Telecommunications Service Priority System

AGENCY: Emergency Communications Division, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

ACTION: 60-Day Notice and request for comments; Extension, 1670-0005

SUMMARY: The Department of Homeland Security (DHS) invites the general public and other federal agencies the opportunity to comment on approved information collection request (ICR) OMB 1670-0005, Telecommunications Service Priority (TSP) System.

DATES: Comments are encouraged and will be accepted until ***[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]***.

ADDRESSES: Interested persons are invited to submit written comments on the proposed information collection to the Office of Information and Regulatory Affairs, Office of Management and Budget. Comments should be sent to tsp@cisa.dhs.gov.

o Federal eRulemaking Portal:

<http://www.regulations.gov>. Please follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name and docket number Docket # CISA-2022-0008. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

SUPPLEMENTARY INFORMATION: TSP is authorized by E.O. 13618 and 47 CFR part 64. The Emergency Communications Division (ECD) of the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), uses the TSP Program to authorize national security and emergency preparedness organizations to receive priority treatment for vital voice and data circuits or other telecommunications service, under National Security or Emergency Preparedness telecommunications (NS/ EP). The TSP Program provides service vendors a Federal Communications Commission (FCC) mandate to prioritize requests by identifying those services critical to national security and emergency preparedness. A TSP assignment ensures that it will receive priority attention by the service vendor before any non-TSP service.

Four broad categories serve as guidelines for determining whether a circuit or telecommunications service is eligible

for priority provisioning or restoration. TSP service user organizations may be in the Federal, State, local, or tribal government, critical infrastructure sectors in industry, non-profit organizations that perform critical NS/EP functions, or foreign governments. Typical TSP service users are responsible for the command-and-control functions critical to management of and response to NS/ EP situations, particularly during the first 24 to 72 hours following an event.

Information to request a priority, to obtain a sponsor for requesting a priority, and for other administrative requirements of the program is required from any person or organization having an NS/EP service for which they wish priority restoration from the vendor providing the service. Information is also required to allow immediate installation of a new service to support NS/EP requirements. Information is required from vendors to allow the ECD to track and identify the telecommunications services that are being provided priority treatment.

The forms used are the SF314 (Revalidation for Service Users), SF315 (TSP Request for Service Users), SF317 (TSP Action Appeal for Service Users), SF318 (TSP Service Confirmation for Service Vendors), and the SF319 (TSP Service Reconciliation for Service Vendors). The SF314 is for users to request that their existing TSP codes be revalidated for three more years. The SF315 is used to

request restoration and/or provisioning for an organization's critical circuits. The SF317 is for organizations to appeal the denial of TSP restoration and/or provisioning. The SF318 is for service vendors to provide circuit ID information associated with TSP codes they've been given by their customers. The SF319 is for service vendors to provide data to the program office in order to reconcile their TSP data with the TSP database. Participants request TSP priorities via email in order to reduce the use of the paper forms. The paper forms will also be available for download via the CISA website. There have been no changes to the information being collected. The annual government cost has increased due to increased wage rates/compensation factors and IT system security requirements. This is a renewal of an information collection.

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the

methodology and assumptions used;

3. Enhance the quality, utility, and clarity of the information to be collected; and

4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

ANALYSIS:

AGENCY: Cybersecurity and Infrastructure Security Agency
(CISA), Department of Homeland Security (DHS)

Title: Telecommunications Service Priority System

OMB Number: 1670-0005

Frequency: Information is required when an organization decides they want TSP priority on their critical circuits. These requests are situational and made at the discretion of the telecommunications user therefore the program office is not able to determine when or how often such requests will occur.

Affected Public: State, Local, Tribal, and Territorial Governments and Private Sector

Number of Respondents: 25,911

Estimated Time Per Respondent: 0.28 hours
Total Annualized Burden Hours: 7,165 hours
Total Annualized Respondent Opportunity Cost: \$372,408
Total Annualized Government Cost: \$1,145,896

Robert J. Costello,
Chief Information Officer,
Department of Homeland Security,
Cybersecurity and Infrastructure Security Agency.
[FR Doc. 2023-07457 Filed: 4/7/2023 8:45 am; Publication Date: 4/10/2023]